

COPY

FILED

12 NOV -5 PM 3:37

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

BY: _____

CARNEY WILLIAMS BATES
PULLIAM & BOWMAN, PLLC
Hank Bates (Ca. # 167688)
hbates@carneywilliams.com
11311 Arcade Drive, Suite 200
Little Rock, Arkansas 72212
Tel: 501-312-8500

MILSTEIN ADELMAN, LLP
Gillian L. Wade, State Bar No. 229124
gwade@milsteinadelman.com
M. Isaac Miller, State Bar No. 266459
imiller@milsteinadelman.com
2800 Donald Douglas Loop North
Santa Monica, CA 90405
Tel: 310-396-9600

Attorney for Plaintiffs Benjamin
Bell and Christopher Spellman, on
behalf of themselves and all others
similarly situated

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CV12-09475 SVW (PJW x)

BENJAMIN BELL and
CHRISTOPHER
SPELLMAN,

Plaintiffs,

vs.

BLIZZARD ENTERTAINMENT,
INC., a Delaware corp., and
ACTIVISION BLIZZARD, INC., a
Delaware corp.

Defendants

) Case No.:

) CLASS ACTION COMPLAINT

) JURY TRIAL DEMANDED

1 **COMPLAINT**

2 Come now the Plaintiffs, Benjamin Bell and Christopher Spellman
3 (“Plaintiffs”), acting individually and on behalf of all other persons similarly situated,
4 and for their Complaint and demand for jury trial state and allege as follows:

5 **INTRODUCTION**

6 1. Plaintiffs bring this action as a class action pursuant to Rules 23(a), (b)(1),
7 (b)(2) and (b)(3) of the Federal Rules of Civil Procedure on behalf of all persons
8 throughout the nation who were deceptively and unfairly sold video game products by
9 Defendants, only to learn after the point of sale that they must purchase additional
10 products from Defendants in order to have even minimal protection for their sensitive
11 personal, private, and financial data (“Private Information”); and whose Private
12 Information was negligently, deliberately, and/or recklessly allowed to be stolen from
13 Blizzard Entertainment and Activision Blizzard (“Defendants”). Plaintiffs’ claims
14 relate to, and arise from, acts of theft, invasion of privacy, and unauthorized use.
15 Plaintiffs seek injunctive relief, compensatory damages, restitution, disgorgement, and
16 recovery of attorneys’ fees and litigation costs.

17 2. Specifically, Plaintiffs assert that (1) Defendants have failed to take the
18 necessary measures to secure the Private Information of their customers, as stored on a
19 website owned and administered by Defendants; (2) as a result of this deficient
20 security, Defendants’ website has suffered multiple instances of theft of the Private
21 Information of its customers; and (3) Defendants have added extra, hidden, post-sale
22 costs onto their products, namely in the form of auxiliary security devices that
23 customers must purchase to ensure the sanctity of their Private Information when
24 using Defendants’ products.

25 3. Defendants are video game manufacturers whose business model is
26 premised on the collection and storage of the Private Information of their customers,
27 via a website called Battle.net. Defendants negligently, deliberately, and/or recklessly
28 fail to ensure that adequate, reasonable procedures safeguard the Private Information

1 stored on this website. As a result of these acts, the Private Information of Plaintiffs
2 and Class members has been compromised and/or stolen since at least 2007. Most
3 recently, on or about May 19, 2012, reports proliferated that Class members'
4 Battle.net accounts had suffered a security breach ("hack") at the hands of unknown
5 parties ("hackers"), and on or about August 4, 2012, hackers massively breached
6 Battle.net's security and acquired the Private Information of all of Defendants'
7 customers in the United States, as well as the remainder of North America, Latin
8 America, Australia, New Zealand, and Southeast Asia.

9 4. In the wake of the hack occurring on or about August 4, 2012,
10 Defendants have not taken the legally required steps to alert Plaintiffs and Class
11 members of the very existence of the hack, and thus have actively impaired Plaintiffs
12 and Class members from taking any meaningful steps to protect their Private
13 Information on their own.

14 5. Defendants' acts have not only harmed Plaintiffs and Class members by
15 subjecting their Private Information to hackers, they have harmed Plaintiffs and Class
16 members by devaluing their video games – purchased from Defendants under certain
17 assurances of security – by adding elements of risk to each and every act of playing
18 said games.

19 6. Moreover, rather than shouldering the burden of adopting sufficient
20 security measures to prevent these repeated hacks and to protect the Private
21 Information of their customers, Defendants instead have informed their customers,
22 after the point of sale, that they must purchase additional security products in order to
23 ensure the sanctity of their Private Information. These additional, post-purchase costs
24 for security products – which Defendants assert are the only measures that may be
25 taken to ensure something even approximating account security when playing their
26 video games – were not disclosed to Plaintiffs and Class members prior to the
27 purchase of Defendants' products.

28 7. Defendants' actions constitute violations of multiple consumer protection

1 statutes, and subject Defendants to additional liability under common law theories of
2 negligence, breach of contract and unjust enrichment.

3 8. Plaintiffs seek damages suffered as a result of Defendants' practices,
4 including, but not limited to, compensatory damages and injunctive relief.

5 **PARTIES AND JURISDICTION**

6 9. Plaintiff Bell is an individual and a citizen of Little Rock, Arkansas. On
7 or about May 21, 2012, Plaintiff Bell purchased Diablo III, a video game
8 manufactured by Defendant Blizzard Entertainment, Inc. On or about May 21, 2012,
9 he obtained an account with Battle.net, a website which is owned and administered by
10 Blizzard Entertainment, Inc. Plaintiff Bell has maintained his Battle.net account since
11 that time, keeping said account continually active through the present. At all times
12 relevant to this litigation, Plaintiff Bell's Battle.net account has operated on
13 Defendants' North American servers, and was thus one of the accounts compromised
14 in the data breach occurring on or about August 4, 2012. Plaintiff's Private
15 Information was compromised as a result of said data breach, described herein.
16 Plaintiff Bell has not purchased or otherwise acquired a Battle.net Authenticator.
17 Plaintiff Bell does not use Defendants' Massively Multiplayer Online Role Playing
18 Game products. To date, Plaintiff Bell has not received any form of notice from
19 Defendants regarding the data breach occurring on or about August 4, 2012, and has
20 instead learned of the compromise of his Private Information through third-party
21 sources.

22 10. Plaintiff Spellman is an individual and a citizen of Los Angeles,
23 California. Plaintiff Spellman owns video games manufactured by Defendants in all
24 of Defendants' franchises: Diablo, StarCraft, and World of Warcraft. Plaintiff
25 Spellman has owned games in the World of Warcraft franchise (Defendants'
26 Massively Multiplayer Online Role Playing Game) since November, 2004; has owned
27 games in the StarCraft franchise since July, 2010; and has owned games in the Diablo
28 franchise since on or about May 15, 2012. Since at least November, 2004, Plaintiff

1 Spellman has held an account with Battle.net, a website which is owned and
2 administered by Blizzard Entertainment, Inc. Plaintiff Spellman has maintained his
3 Battle.net account since that time, keeping said account continually active through the
4 present. At all times relevant to this litigation, Plaintiff Spellman's Battle.net account
5 has operated on Defendants' North American servers, and was thus one of the
6 accounts compromised in the data breach occurring on or about August 4, 2012.
7 Plaintiff Spellman's Private Information was compromised as a result of said data
8 breach described herein. Plaintiff Spellman owns at least two Battle.net
9 Authenticators, including a Mobile Authenticator and a Key Ring Authenticator. To
10 date, Plaintiff Spellman has not received any form of notice from Defendants
11 regarding the data breach occurring on or about August 4, 2012, and has instead
12 learned of the compromise of his Private Information through third-party sources.

13 11. Defendant Blizzard Entertainment, Inc. ("Blizzard" or the "Company") is
14 a Delaware corporation headquartered in Irvine, California. Blizzard is a video game
15 developer and publisher.

16 12. Defendant Activision Blizzard, Inc. ("Activision Blizzard") is the
17 American holding company for multiple game-publishing entities, including Blizzard.
18 Activision Blizzard, Inc. is a Delaware corporation, with headquarters in Santa
19 Monica, California.

20 13. The Court has subject matter jurisdiction over this nationwide class
21 action pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of
22 2005, because the matter in controversy exceeds \$5,000,000.00, exclusive of interest
23 and costs, and is a class action in which some members of the Class are citizens of
24 states different than Defendants. *See* 28 U.S.C. § 1332(d)(2)(A). The Court has
25 personal jurisdiction over Defendants because they own and operate businesses that
26 are headquartered in California and conduct substantial business throughout
27 California.

28 14. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b)(1).

1 All Defendants in this action – Defendant Blizzard Entertainment, Inc. and Defendant
2 Activision, Inc. – are headquartered in this district.

3 15. Venue is also proper in this district pursuant to Defendants’ Dispute
4 Resolution Policy, which is part of Defendants’ Terms of Use and End User License
5 Agreement with Plaintiffs, and which states that all court proceedings arising out of
6 disputes between Plaintiffs and Defendants “shall be decided by a court of competent
7 jurisdiction within the County of Los Angeles, State of California, United States of
8 America, and you and Blizzard agree to submit to the personal jurisdiction of that
9 court.”

10 16. Delaware’s law governs the substantive legal issues in the instant matter,
11 as Defendants’ Dispute Resolution Policy, incorporated by reference into all
12 agreements entered into between Plaintiffs and Defendants, expressly provides that
13 Delaware law will govern the Agreement and claims arising from the Agreement.
14 Dispute Resolution Policy at § 6, “Governing Law.” Defendants, as drafters of the
15 Agreement, should be bound by their own terms.

16 **FACTUAL BACKGROUND**

17 17. Defendant Blizzard is an American video game developer and publisher,
18 headquartered in Irvine, California. Among the video game titles that Blizzard
19 publishes and markets are Diablo, Diablo II, Diablo III, and related expansion packs¹
20 (collectively, the “Diablo franchise”); StarCraft, StarCraft II, and related expansion
21 packs (collectively, the “StarCraft franchise”); and World of Warcraft and related
22 expansion packs (collectively, “World of Warcraft”). Costs for the software of the
23 underlying game and related expansion packs typically range in price from \$14.99-
24 \$59.99, although collector’s edition versions of the games cost close to \$200.00.²

25 ¹ An “expansion pack” is a supplement to an already purchased video game, providing players with an extended
26 storyline, along with new characters, objects, and related content. The cost of an expansion pack is usually less than the
27 underlying video game, as are the costs associated with manufacturing the product. Ultimately, expansion packs serve as
28 a way to extend the playing life of a video game, allowing companies to continue earning revenue on a franchise and
allowing players to add hours of gameplay, all after the underlying game has been played all the way through.

² Amazon.com’s list price for the Diablo III Collector’s Edition is \$179.99 (http://www.amazon.com/Diablo-III-Collectors-Edition-Pc/dp/B0050SZC5U/ref=sr_1_2?ie=UTF8&qid=1347373717&sr=8-2&keywords=diablo+III). The list price for the collector’s edition of StarCraft II: Wings of Liberty is \$182.99 (<http://www.amazon.com/Starcraft-II->

1 A. BATTLE.NET ACCOUNTS: CUSTOMERS' PRIVATE
2 INFORMATION BECOMES A REQUISITE OF GAME PLAY;
3 HIDDEN COSTS ARISE.

4 18. Beyond the development and publishing of its video game titles, Blizzard
5 owns and administers Battle.net, a website that manages online accounts for Blizzard
6 customers. Defendants require customers to activate Battle.net accounts in order to
7 play any of the games manufactured and sold by Defendants.

8 19. However, Battle.net accounts only impact game functionality for World
9 of Warcraft players, as this title is a “massively multiplayer online role-playing game”
10 (“MMORPG”), which is played on a computer with an internet connection, allowing
11 players from different physical locations to interact with each other within a virtual
12 game world. Battle.net accounts do not have any bearing on the functionality of
13 games in either the StarCraft or Diablo franchises, as neither of those titles are
14 MMORPGs, and would neither in theory nor in practice require either an internet
15 connection or ancillary Battle.net account in order to be played.

16 20. Instead, the *chief* function of a Battle.net account is to provide
17 Defendants access to account holders’ Private Information and to facilitate the
18 purchase of Defendants’ additional products and services. Battle.net accounts offer a
19 feature called “Battle.net Balance,” which allows account holders to add funds via
20 their credit or debit cards to their Battle.net accounts, which in turn may be used to
21 purchase goods and services from Defendants.³ Most recently, Blizzard has further
22 monetized Battle.net by establishing a “Real Money Auction House” (“RMAH”) in
23 the Diablo franchise, in which players can spend their Battle.net Balance for in-game
24 items like weapons, armor, or “commodities” like gold and gems.⁴ Blizzard charges
25 transaction fees of \$1.00 (USD) for each auction of equipment like weapons and
26 armor, and charges a 15% transaction fee for sales of commodities.

27
28 Liberty-Collectors-Edition-Pc/dp/B002I0JMB8/ref=pd_sim_vg_4)

³ <http://us.battle.net/support/en/article/battle-net-balance-faq#purchase>

⁴ <http://us.battle.net/support/en/article/diablo-iii-auction-house-general-information>

1 **1. Step One in Establishing a Battle.net Account: Relinquishing**
 2 **Personal and Financial Data.**

3 21. In order to obtain a Battle.net account, a customer must provide sensitive
 4 Private Information included, but not limited to, his or her full name, date of birth, and
 5 e-mail address.⁵ Additionally, the customer must choose a “secret question,” to which
 6 he or she provides an answer. The options for the account holder’s “secret question”
 7 are not customizable, and instead consist of generic choices that are the standard
 8 questions used by other, popular websites: “First elementary school I attended;” “The
 9 high school I graduated from;” “Your city of birth;” “Name of your first pet;” “Your
 10 favorite sports team,” among others.

11 22. Where customers obtain a Battle.net Balance to purchase products and
 12 services through the website or to utilize the RMAH, they are prompted to enter even
 13 more Private Information, including their credit card number, credit card expiration
 14 date, billing address, and phone number. All of this information remains stored in the
 15 Battle.net account.

16 23. Defendants make assurances to Battle.net account holders that this
 17 Private Information will remain completely secure. Specifically, the Battle.net Terms
 18 of Use agreement (“Agreement”) requires, as part of its terms, that account holders
 19 agree to be bound by Defendants’ Privacy Policy. Battle.net Terms of Use at § 3,
 20 “Requirements.”

21 24. Defendants’ Privacy Policy states, in pertinent part:

22 **How Secure is My Personal Information?** Blizzard has taken steps
 23 to assure that all information collected will remain secure and in its
 24 original form, *i.e.*, free from any alteration. As such, access to all
 25 Personal Information is strictly controlled. When credit card
 26 information is transmitted, for example, we use industry standard,
 27 SSL (secure sockets layer) encryption. In addition, we will take
 28

⁵ <https://us.battle.net/account/creation/tos.html>

1 reasonable steps to assure that third parties to whom we transfer any
 2 data will provide sufficient protection of Personal Information. We
 3 will retain your information for as long as needed to provide you
 4 services.⁶

5 **2. Step Two in Establishing a Battle.net Account: Paying**
 6 **Additional, Hidden Costs to Protect One's Private**
 7 **Information.**

8 25. While Defendants do inform customers, on the video game's box, that
 9 Battle.net accounts are required in order to play any of Defendants' titles, it is not
 10 until after a customer purchases the video game and establishes a Battle.net account
 11 that he or she learns that it is also necessary to purchase an additional product in order
 12 to ensure adequate security of the Private Information stored in the Battle.net account
 13 and to access certain features of game play. Specifically, customers learn that they
 14 must purchase a product called a Battle.net Authenticator ("Authenticator"). In the
 15 Battle.net Terms of Use agreement ("T.O.U."), section 6, subsection B, in all caps,
 16 customers are informed that "IN ORDER TO USE THE BATTLE.NET BALANCE
 17 FEATURE, YOU MUST ATTACH A BATTLE.NET AUTHENTICATOR TO
 18 YOUR ACCOUNT" (available at [http://us.blizzard.com/en-](http://us.blizzard.com/en-us/company/about/termsfuse.html)
 19 [us/company/about/termsfuse.html](http://us.blizzard.com/en-us/company/about/termsfuse.html)).

20 26. Introduced in 2008,⁷ an Authenticator is a device that generates a random
 21 code, which Battle.net account holders are prompted to enter in addition to their
 22 password. "By using an authenticator," Blizzard promises, "access to a Battle.net
 23 account is restricted to only individuals with the authenticator code, helping prevent
 24 unauthorized access."⁸

25 27. Authenticators come in two varieties: a physical, keychain authenticator
 26 ("Key Ring Authenticator") and an authenticator app that is downloadable onto a

27 ⁶ <http://us.blizzard.com/en-us/company/about/privacy.html>

28 ⁷ Daniel Whitcomb, *Blizzard Authenticator to be Introduced at the Worldwide Invitational*, WoW Insider (June 26, 2008) (available at <http://wow.joystiq.com/2008/06/26/blizzard-authenticator-to-be-introduced-at-the-worldwide-invitat/>)

⁸ <https://us.battle.net/support/en/article/battlenet-authenticator>

customer's smart phone ("Mobile Authenticator"). The Key Ring Authenticator costs \$6.50,⁹ while the cost for a Mobile Authenticator varies depending upon the mobile device.¹⁰ Upon information and belief, as of December, 2011, Defendants generated \$26 million on Authenticator sales.¹¹

28. Ultimately, as discussed in paragraph 37, *infra*, the \$6.50 Key Ring Authenticator is currently the only viable option for maintaining account security, as the security of the Mobile Authenticators was compromised following a Battle.net data breach occurring on or about August 4, 2012. Thus, any of Defendants' customers who wish to (1) use the entirety of the features available in the video game that they purchased, and (2) protect the Private Information stored in their mandatory Battle.net accounts, must pay further, undisclosed, after-purchase costs of \$6.50 for the Key Ring Authenticator.

**B. BATTLE.NET ACCOUNTS ARE REPEATEDLY
COMPROMISED, JEOPARDIZING ACCOUNT HOLDERS'
PRIVATE INFORMATION. DEFENDANTS BLAME THE
CUSTOMERS, TELLING THEM TO SPEND MORE MONEY TO
ENSURE ACCOUNT SECURITY.**

**1. Battle.net Accounts are Hacked on May 19, 2012; Defendants
Admit That "Players Have Been Seeing This For Five Years
Or So".**

29. On or about May 19, 2012, Blizzard began to receive reports from players of the Diablo franchise that their Battle.net accounts were being hacked, with items such as gold and characters going missing from the customers' accounts.¹² The phenomenon was widespread, and profoundly upsetting to players, who had seen tens

⁹ <http://us.blizzard.com/store/details.xml?id=1100001981>

¹⁰ <https://us.battle.net/support/en/article/battle-net-mobile-authenticator-faq>. See Subsection "Why does the Battle.net Mobile Authenticator cost different amounts for different mobile devices?"

¹¹ Matthew Humphries, *Blizzard Has Made \$26 Million Just From Battle.net Authenticators*, Geek.com (Dec. 30, 2011) (available at <http://www.geek.com/articles/games/blizzard-has-made-26-million-just-from-battle-net-authenticators-20111230/>)

¹² Nathan Grayson, *Shout at the Devil: Blizzard Aware of Diablo III Hacks*, Rock, Paper, Shotgun. (May 21, 2012) (available at <http://www.rockpapershotgun.com/2012/05/21/shout-at-the-devil-blizzard-acknowledges-diablo-iii-hacks/>).

1 or even hundreds of hours' worth of game play erased, with one commentator likening
2 it to "walking into your house after a robbery."¹³

3 30. Responding to angry customers, one of Defendants' support agents,
4 Kaltonis replied that these security breaches in Battle.net accounts for the Diablo
5 franchise were "no different than what World of Warcraft players have been seeing
6 *for five years or so.*"¹⁴ (emphasis added). Kaltonis went on to say that the fix for this
7 problem was the purchase of an Authenticator, stating "[i]f you have the physical or
8 mobile authenticator (both of which major banks use and charge \$30+ for) the chances
9 of you being compromised are very, very small."

10 31. Thus, instead of responding by fixing their internal security protocols, as
11 promised in Defendants' Privacy Policy, *supra*, or by taking *any* remedial measures
12 that did not result in increased costs to account holders, Defendants first told
13 customers that these problems were systemic, and had been going on for five years,
14 and then told their customers that the only way to keep their accounts secure was
15 through the additional purchase of an Authenticator to the Battle.net account.
16 Defendants' official response to customers, posted on their website on May 21, 2012,
17 conceded:

18 Historically, the release of a new game -- such as a World of
19 Warcraft® expansion -- will result in an increase in reports of
20 individual account compromises, and that's exactly what we're seeing
21 now with Diablo III. We know how frustrating it can be to become
22 the victim of account theft, and as always, we're dedicated to doing
23 everything we can to help our players keep their Battle.net accounts
24 safe -- and we appreciate everyone who's doing their part to help
25 protect their accounts as well.

26
27 ¹³ Paul Tassi, *The Horror of Being Hacked in Diablo 3*, Forbes (May 30, 2012) (available at
<http://www.forbes.com/sites/insertcoin/2012/05/30/the-horror-of-being-hacked-in-diablo-3/>).

28 ¹⁴ William Usher, *Blizzard Admits Accounts with Authenticators Have Been Hacked*, Gaming Blend (May 25, 2012)
(available at <http://www.cinemablend.com/games/Blizzard-Admits-Accounts-With-Authenticators-Have-Been-Hacked-42909.html>).

We also wanted to reassure you that the Battle.net Authenticator and Battle.net Mobile Authenticator (a free app for iPhone and Android devices) continue to be some of the most effective measures we offer to help players protect themselves against account compromises, and we encourage everyone to take advantage of them.¹⁵

32. In all subsequent discussions of the hack, Defendants consistently returned to the refrain, equating Authenticators with account security. For instance, Defendants' community manager, Bashiok responded to complaints on a Battle.net forum by stating, "We have yet to investigate a compromise report in which an authenticator was attached beforehand."¹⁶

33. Defendants also created a "security checklist" for players, which reads in the following order:

- ***Add a Battle.net Authenticator to your account. Seriously.***
- Update your browser to the latest version.
- Activate your browser's phishing filter.
- Make sure your registered email address is secure and up-to-date.
- Make sure your computer operating system is up-to-date.
- Make sure your browser plug-ins and other commonly used applications are up-to-date.
- Install anti-virus software.
- Learn to identify common types of account theft.
- Keep in mind the list of safe, official Blizzard Entertainment domains.¹⁷

(Emphasis added). Thus, beyond telling Class members to tighten up their *own* internet security protocols in order to keep their accounts safe, Defendants' very first

¹⁵ <http://us.battle.net/d3/en/forum/topic/5149619846#1>

¹⁶ Kevin Parrish, *Blizzard Responds to Diablo 3 Account Hack*, Tom's Hardware (May 22, 2012) (available at <http://www.tomshardware.com/news/Diablo-3-Authenticator-Battle.net-Bashiok-Password,15724.html>).

¹⁷ <http://us.battle.net/en/security/checklist>

1 remedial measure suggested was, “seriously,” to buy an additional product from
2 Defendants: an Authenticator.

3 34. Customers were understandably enraged that Defendants placed the onus
4 for account security on the victim of the security breach. An article in Forbes
5 magazine, decrying this practice, noted:

6 [I]f the authenticator is the end-all, be-all of keeping your account
7 safe, then shouldn't it be standard with every new account made?
8 Blizzard tries to sell the physical product at cost, but it seems like it
9 should be included in every box copy, or required as a free download
10 if it truly is the final answer to keep an account safe. If a \$5 keyfob
11 [sic] is what it takes to make their game secure, Blizzard should be
12 eating that cost, not the player.¹⁸

13 **2. Defendants' Largest Breach To Date: August 4, 2012.**

14 35. The need for increased account security was driven home again 2 months
15 later, on or about August 9, 2012, with media outlets reporting that Blizzard had
16 revealed on its company website¹⁹ that account details for millions of customers had
17 been stolen by hackers, as a result of an attack on Battle.net.²⁰ While Defendants'
18 post made no mention of the date of the attack, news reports state that Blizzard was
19 aware of the data breach as early as August 4, 2012.²¹

20 36. Concerning the scope of compromised customer data, the Company
21 stated that “for players on North American servers (which generally includes players
22 from North America, Latin America, Australia, New Zealand, and Southeast Asia),”
23 the hackers had gained access to email addresses, answers to personal security
24 questions, and “cryptographically scrambled versions of Battle.net passwords.”²²

25 ¹⁸ Paul Tassi, *For Diablo 3 Hacking, the Buck Stops Where?*, Forbes (May 31, 2012) (available at
26 <http://www.forbes.com/sites/insertcoin/2012/05/31/for-diablo-3-hacking-the-buck-stops-where/>).

¹⁹ <http://sea.blizzard.com/en-sg/securityupdate.html>

27 ²⁰ *Blizzard Battle.net Hack Attack Hits Millions*, BBC (Aug. 10, 2012) (available at
<http://www.bbc.com/news/technology-19207276>).

28 ²¹ Kyle Orland, *Hackers Collect Significant Account Details From Blizzard Servers*, Ars Technica (Aug. 9, 2012)
(available at <http://arstechnica.com/gaming/2012/08/hackers-collect-significant-account-details-from-blizzard-servers/>).

²² <http://sea.blizzard.com/en-sg/securityupdate.html>

1 37. Additionally, Defendants stated that “[w]ith regard to Mobile
2 Authenticators, information was taken that could potentially compromise the integrity
3 of North American Mobile Authenticators.”²³ Thus, as a result of this data breach, in
4 order to be assured of *any* modicum of security through the use of an Authenticator, a
5 consumer would be burdened by the additional expense of a Key Ring Authenticator,
6 on top of any money already spent on a now worthless Mobile Authenticator.

7 38. In its Battle.net post, Blizzard stated that “Based on what we currently
8 know, this information alone is NOT enough for anyone to gain access to Battle.net
9 accounts.”²⁴

10 39. This proposition was immediately challenged, however. Within 24 hours
11 of Blizzard’s statement, one tech industry executive published a series of pieces
12 explaining that the Company’s mechanism for protecting users’ passwords—Secure
13 Remote Password protocol (“SRP”)—was insufficient.²⁵ Specifically, the author
14 noted that the SRP server-side verifier database (“verifier database”) was also stolen
15 in the hack.

16 40. Where thieves possess (1) an encrypted version of the password and (2)
17 the verifier database, they will be able to employ what is known as a “dictionary
18 attack,” which effectively cross-checks the password against all likely possibilities
19 from an exhaustive list of possible values (called a “dictionary”).

20 41. The author of the pieces stated that, based upon the data obtained in the
21 Battle.net hack, each password could be individually attacked at a rate of 100,000
22 guesses per second. By this estimate, the thieves could “reasonably check 100,000 of
23 their top passwords against 400,000 usernames, per day,” and accordingly “[s]ince the
24 attack occurred, millions of users’ passwords have likely already been cracked.”²⁶

25 ²³ <https://us.battle.net/support/en/article/important-security-update-faq>

26 ²⁴ *Id.*

27 ²⁵ Jeremy Lippman, *SRP Won’t Protect Blizzard’s Stolen Passwords* (Aug. 9, 2012) (available at
<http://www.opine.me/blizzards-battle-net-hack/>); See also Dan Goodin, *Why Hacked Blizzard Passwords Aren’t as Hard*
28 *to Crack as Company Says*, Ars Technica (Aug. 13, 2012) (available at <http://arstechnica.com/security/2012/08/hacked-blizzard-passwords-not-hard-to-crack/>).

²⁶ Jeremy Lippman, *SRP Won’t Protect Blizzard’s Stolen Passwords* (Aug. 9, 2012) (available at
<http://www.opine.me/blizzards-battle-net-hack/>)

42. Beyond obtaining users' passwords via dictionary attacks, a prospective identity thief could use a much simpler technique known as "phishing," in which the thief sends an email that looks like an official communication from the hacked company (in this case, Blizzard), seeking verification of a password or other sensitive information like a credit card number. The unsuspecting recipient believes that they are simply updating information at the request of the company, when in fact they are providing a data thief with sensitive, Private Information. Numerous news outlets and publications dedicated to web security have stated that the Battle.net data breach puts Blizzard customers at dramatically increased risk of phishing attacks targeting the compromised email addresses.²⁷

43. Whether obtaining access to customer accounts via dictionary attacks on stolen passwords or through phishing attacks on stolen e-mails, hackers *have* obtained illegal access to Battle.net accounts, following the data breach of August 4, 2012. Blizzard's customer support service ("Customer Support"), which maintains a Twitter feed that makes customer service requests viewable over the Web, reveals that multiple conversations occurred between Battle.net account holders and Customer Support, where account holders have been locked out of their accounts following the August 4, 2012 data breach (see attached Exhibit A). In many of these exchanges, Customer Support acknowledges the account being "compromised," and also acknowledges the data breach.

44. Similarly, since the August 4, 2012 data breach, customers have posted, on forums throughout the Internet, comments to the effect that their Battle.net accounts have been frozen or otherwise stolen as a result of the breach.²⁸

B. IN ITS POST-DATA-BREACH ACTIONS, BLIZZARD HAS

²⁷ See, e.g., Todd Kenreck, *Blizzard's Network of More Than 10 Million Hacked*, NBC News (Aug. 10, 2012) (available at <http://www.nbcnews.com/technology/ingame/blizzards-network-more-10-million-hacked-933846>); *Online Entertainment Caught in Blizzard of Hacks*, Simply Security (Aug. 17, 2012) (available at <http://www.simplysecurity.com/2012/08/17/online-entertainment-caught-in-blizzard-of-hacks/>); Charles Arthur, *Diablo and World of Warcraft Players Warned Over Battle.net Hacking*, The Guardian (Aug. 10, 2012) (available at <http://www.guardian.co.uk/technology/2012/aug/10/diablo-world-of-warcraft-hacking>).

²⁸ See, e.g., http://www.reddit.com/r/gaming/comments/ybx48/my_battlenet_account_was_stolen_does_anyone_have/

**FAILED TO PROVIDE MEANINGFUL WARNING TO
BATTLE.NET ACCOUNT HOLDERS.**

45. Upon information and belief, the only affirmative steps that Blizzard has taken to inform Battle.net account holders that their Private Information has been stolen are confined to posts on Blizzard's website (and not Battle.net). Upon information and belief, Battle.net account holders have not been notified via phone, email, letter or any other medium that their accounts have been compromised and their information has been stolen. Instead, the massive, continent-spanning data breach, resulting in the theft of Private Information of millions of people, was merely announced as a post on Defendants' website – a location to which few, if any, of its customers would travel.

46. Further, upon information and belief, for a period of time following the August 4, 2012, data breach, a customer who logged in to his or her Battle.net account could not even change his or her account details. As detailed in attached Exhibit B, as of 12:53 PM, CST, August 28, 2012, where a customer logged in to the Battle.net website, and attempted to access account information (including Private Information), the user was redirected to a screen that read "We'll be back soon! The Blizzard family of websites is currently undergoing maintenance to improve your browsing experience. Thank you for your patience!" followed by a prompt to follow Blizzard on Twitter, a popular social media website.

47. Accordingly, unless a Blizzard customer either stumbles across a news story detailing the data breach or Blizzard's post on his or her own, or attempts to log in to an account that has already been hacked, he or she will have had *no notice* that Private Information has been stolen.

48. Moreover, where a Blizzard customer did learn of the attack on Battle.net, and wished to change the details of his or her account in order to remove credit card information or other sensitive data, the Company had made that impossible due to its "maintenance to improve [the] browsing experience," at least as late as

1 August 28, 2012. It should be noted that, at some point between August 28 and
2 September 6, 2012, Battle.net accountholders were finally able to amend the Private
3 Information in their accounts.

4 49. Accordingly, for a significant period following the August 4, 2012 data
5 breach, until some point between August 28 and September 6, 2012, *a customer could*
6 *take no affirmative steps to protect his or her personal and financial information, as a*
7 *result of Defendants' actions.*

8 **C. DEFENDANTS' ACTIONS HAVE HARMED PLAINTIFFS AND**
9 **CLASS MEMBERS.**

10 50. At all relevant times, Plaintiffs have owned games manufactured by
11 Defendants and have had Battle.net accounts.

12 51. Defendants have consistently misrepresented the quality and reliability of
13 the Battle.net website, along with their ability to keep the Private Information of
14 Plaintiffs and Class members secure. Such misrepresentations include, *inter alia*,
15 statements made in Defendants' Privacy Policy, provided at the point of purchase of
16 Defendants' video games.

17 52. Upon information and belief, Defendants have failed, at all times relevant
18 to this litigation, to disclose to Plaintiffs and Class members prior to the point of sale
19 the necessity of a post-point-of-sale purchase of an Authenticator, at \$6.50, for
20 purposes of using the Battle.net Balance feature of their Battle.net accounts, for
21 ensuring the security of the Private Information in their Battle.net accounts, or for any
22 other purpose.

23 53. Upon information and belief, Defendants failed to maintain proper
24 security protocols to prevent the theft of Private Information of Class members.

25 54. Upon information and belief, Defendants had been placed on notice that
26 Battle.net was vulnerable to widespread hacking since as early as 2007, according to
27 statements made by Defendants' employee, Kaltonis. *See* paragraph 27, *supra*.

28 55. Despite having five years' notice of account vulnerabilities, Defendants

1 *continued* to fail to take adequate security precautions, resulting in a massive data
2 breach on or about August 4, 2012, at which point the Private Information of Plaintiffs
3 and Class members was again compromised.

4 56. Further, Defendants have duplicitously failed to alert Plaintiffs and Class
5 members of, at the minimum, the data breach occurring on or about August 4, 2012.
6 Upon information and belief, Defendants have not provided notice, either in written,
7 telephonic, or electronic form, to any of their customers, including Plaintiffs and Class
8 members, alerting them to the breach.

9 57. Moreover, upon information and belief, Defendants made it impossible to
10 edit one's Battle.net account details, in turn making it impossible for an account
11 holder, including Plaintiffs and Class members, to remove his or her credit card
12 information (and thus take affirmative steps to actually protect Private Information).

13 58. As discussed in paragraph 43, *supra*, upon information and belief,
14 members of the Class have begun to experience losses from fraudulent use of the
15 Private Information obtained as a result of the August 4, 2012 data breach.

16 59. Defendants' deceptive and negligent behavior, engaged in wantonly,
17 purposely, and recklessly, has put the Private Information of Plaintiffs and Class
18 members at continual risk. Such behavior, and its attendant consequences, has
19 deprived Plaintiffs and Class members of the full value of all goods and services
20 purchased from Defendants. As the months have unfolded in 2012, and as the
21 instances of reported security lapses mount, it becomes more and more evident that
22 playing games manufactured by Defendants – games that can cost almost \$200 –
23 requires gambling with the sanctity and security of one's Private Information,
24 including, but not limited to, one's name, address, and credit card information. Any
25 game, the playing of which is conditioned upon such a risk, becomes devalued. As
26 the data breaches mount, the value decreases further.

27 **CLASS ACTION ALLEGATIONS**

28 60. This action is brought on behalf of Plaintiffs, individually, and as a class

1 action, on behalf the following classes (collectively referred to as “the Class” or
2 “Class”)²⁹

3 a. **The Authenticator Class:** All residents of the United States who
4 purchased a video game manufactured by Defendants, after the
5 introduction of the Authenticator for post-sale purchase in 2008.

6 b. **The August 4 Class:** All residents of the United States whose Private
7 Information was stolen from the Defendants’ Battle.net website as a
8 result of the data breach on or about August 4, 2012.

9 61. The Class does not include Defendants, or their officers, directors,
10 agents, or employees.

11 62. Plaintiffs reserve the right to modify or amend the definition of the Class
12 before the Court determines whether certification is appropriate.

13 63. The members of the Class are so numerous that joinder is impractical.
14 The Class consists of at least ten million members, the identity of whom, upon
15 information and belief, is within the knowledge of Defendants and can be ascertained
16 only by resort to Defendants’ records.

17 64. The representative Plaintiffs’ claims are typical of the claims of the
18 members of the Class in that (1) they, like all members of the Class, maintained
19 Battle.net accounts prior to, during, and following the August 4, 2012, data breach,
20 and had Private Information stolen as a result of Defendants’ negligent, deliberate,
21 and/or reckless behavior; and (2) purchased Defendants’ video games and were not
22 informed, at the point of sale, that an Authenticator would be required to either
23 acquire a Battle.net Balance or ensure the security of the Private Information stored on
24 their Battle.net accounts.

25 65. Questions of law and fact common to the Class predominate over
26 questions that may affect individual Class members, including, *inter alia*:

27
28 ²⁹ There is significant overlap between the Authenticator Class and the August 4 Class, as all of Defendants customers who maintained an active Battle.net account during the data breach occurring on or about August 4, 2012 are members of both classes.

- a. Whether Defendants concealed and did not disclose at the point of purchase the fact that Plaintiffs and Class members would need make additional purchases, in the form of Authenticators;
- b. Whether Defendants concealed and did not disclose the deficiencies in the security protocols of the Battle.net accounts of Plaintiffs and Class members;
- c. Whether Defendants misrepresented their ability to protect Private Information contained the in Battle.net accounts of Plaintiffs and Class members;
- d. Whether Defendants failed to provide reasonable notification to Battle.net account holders, alerting them of the August 4, 2012 data breach;
- e. Whether Defendants' conduct constitutes an unfair and/or deceptive trade practice;
- f. Whether Defendants' conduct constitutes a breach of its contract with Plaintiffs and Class members;
- g. Whether Defendants owed a duty to Plaintiff and/or the Class to protect their Private Information;
- h. Whether Defendants took reasonable measures to safeguard consumers' Private Information;
- i. Whether Defendants were negligent in collecting and storing the Private Information of Plaintiffs and Class members;
- j. Whether Defendants were negligent in failing to keep Plaintiff and Class members' Private Information secure;
- k. Whether Defendants breached their duty to exercise reasonable care in storing consumers' Private Information by storing that information on their computer systems and in their physical possession;
- l. Whether Defendants breached a duty by failing to keep Plaintiff and

1 Class members' Private Information secure;

2 m. Whether Plaintiff and members of the Class have sustained damages, and
3 if so, what is the proper measure of those damages; and

4 n. Whether injunctive relief is appropriate in this matter.

5 66. Plaintiffs will fairly and adequately represent and protect the interests of
6 the Class, in that they have no interest that is antagonistic to, or that irreconcilably
7 conflicts with, those of other members of the Class.

8 67. Plaintiffs have retained counsel competent and experienced in the
9 prosecution of class action litigation.

10 68. A class action is superior to all other available methods for the fair and
11 efficient adjudication of Plaintiffs' and the Class members' claims. Plaintiffs and the
12 members of the Class have suffered irreparable harm as a result of Defendants'
13 deceptive, intentional, reckless, negligent, and unlawful conduct. The damages
14 suffered by individual Class Members may be relatively small, and thus few, if any,
15 individual class members can afford to seek legal redress on an individual basis for the
16 wrong complained of herein. Absent a class action, Plaintiffs and members of the
17 Class will continue to suffer losses as a result of Defendants' unlawful and negligent
18 conduct.

19 COUNT I

20 **Violation of Delaware's Consumer Fraud Act ("CFA") 6 Del. C. § 2511 *et seq.***

21 **(On Behalf of the Authenticator Class)**

22 69. Plaintiffs repeat all paragraphs above.

23 70. The goods and services provided by Defendants to Plaintiffs and all other
24 Authenticator Class members constitute "merchandise" within the meaning of the
25 CFA.

26 71. By reason of the conduct alleged herein, Defendants engaged in
27 violations of the CFA where they employed "deception, fraud, false pretense, false
28 promise, misrepresentation, or the concealment, suppression, or omission of any

1 material fact with intent that others rely upon such concealment, suppression or
2 omission, in connection with the sale, lease or advertisement of any merchandise.” 6
3 Del. C. § 2513(a).

4 72. Defendants violated the CFA—and continue to violate the CFA—by
5 failing to inform consumers, at the initial point of sale of Defendants’ video games,
6 that a Battle.net Authenticator is necessary to ensure any modicum of security for
7 Battle.net accounts. This amounts to an undisclosed, after-the-fact charge that
8 consumers are required to pay, simply to prevent their Battle.net accounts from being
9 hacked while they play video games for which they have already paid as much as
10 \$182.99. If Battle.net account holders do *not* purchase these items, their Private
11 Information is subjected to a drastically increased risk of being stolen, a fact that
12 customers are made privy to only following the purchase of their games and the
13 establishment of their Battle.net accounts. On information and belief, over \$26
14 million has been spent by class members on authenticators.

15 73. Defendants violated the CFA—and continue to violate the CFA—by
16 failing to disclose, at the point of purchase of the video games they manufacture and
17 distribute, that in order to obtain a Battle.net account and actually use Defendants’
18 games, the consumer must (1) provide Private Information, and (2) expose said
19 Private Information to increased risk of theft unless the consumer makes a subsequent
20 purchase of a Battle.net authenticator.

21 74. Defendants’ omissions, misrepresentations and other conduct induced
22 Plaintiffs and Authenticator Class members to purchase Defendants’ products under
23 the assumption, at the point of sale, that no additional purchase of an Authenticator or
24 any other product or service would be necessary to ensure the account security
25 warranted by Defendants in, *inter alia*, Defendants’ Privacy Policy.

26 75. As a result of Defendants’ violations of the CFA, Plaintiffs and all other
27 Class members are entitled to compensatory damages and injunctive relief.
28

COUNT II

Violation of Delaware’s Consumer Fraud Act (“CFA”) 6 Del. C. § 2511 *et seq.*

(On Behalf of the August 4 Class)

Plaintiffs repeat all paragraphs above.

76. The goods and services provided by Defendants to Plaintiffs and August 4 Class members constitute “merchandise” within the meaning of the CFA.

77. By reason of the conduct alleged herein, Defendants engaged in violations of the CFA where they employed “deception, fraud, false pretense, false promise, misrepresentation, or the concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale, lease or advertisement of any merchandise.” 6 Del. C. § 2513(a).

78. Defendants violated the CFA—and continue to violate the CFA—by misrepresenting the quality of their security protocols for Battle.net, and by misrepresenting their ability to safely store customers’ Private Information. Defendants stated, in Battle.net’s Privacy Policy, that account holders could be “assure[d] that all information collected will remain secure” and that “access to all Private Information is strictly controlled.” Defendants failed, however, to keep such information secure and strictly controlled, as evidenced not only by the data breach occurring on or about August 4, 2012, but also the account hacks occurring, by Defendants’ own admission, as early as 2007.

79. Defendants violated the CFA—and continue to violate the CFA—by failing to disclose, at the point of purchase of the video games they manufacture and distribute, that in order to obtain a Battle.net account and actually use Defendants’ games, the consumer must (1) provide Private Information, and (2) expose said Private Information to increased risk of theft unless the consumer makes a subsequent purchase of a Battle.net authenticator.

80. Defendants’ omissions, misrepresentations and other conduct induced

1 Plaintiffs to obtain Battle.net accounts and to provide Private Information when
2 registering for Battle.net accounts. But for these actions, Plaintiffs and all other
3 August 4 Class members would not have had their Private Information compromised,
4 which event resulted in (1) the loss of the unencumbered use of their passwords; (2)
5 the procurement, by hackers, of their Private Information without their consent; and
6 (3) the inability to take steps to protect themselves and their Private Information.

7 81. Defendants further violated the CFA—and continue to violate the CFA—
8 by failing to immediately notify Plaintiffs and all other August 4 Class members of
9 the August 4, 2012 data breach. Moreover, to date, Defendants have taken no
10 meaningful steps to alert Plaintiffs and all other August 4 Class members of the data
11 breach.

12 82. Such concealment and failure to act amounts to a violation of 6 Del. C. §
13 12B-101, *et seq.*

14 83. Defendants are a “commercial entity,” within the meaning of Delaware’s
15 data breach notification laws, as defined in 6 Del. C. § 12B-101.

16 84. The data breach occurring on or about August 4, 2012, constituted a
17 “breach of the security system” of Defendants, within the meaning of Delaware’s data
18 breach notification laws, as defined in 6 Del. C. § 12B-101.

19 85. Under Delaware’s data breach notification laws, where Defendants
20 became aware that the Private Information of Plaintiffs and all other August 4 Class
21 members had been compromised as a result of the data breach occurring on or about
22 August 4, 2012, Defendants had a duty to give notice “as soon as possible” to all
23 affected Battle.net account holders. Upon information and belief, Defendants have
24 failed, to date, to provide any notice to Plaintiffs and all other members of the August
25 4 Class, let alone to provide notice in a manner consistent with the requirements of 6
26 Del. C. § 12B-102(3).

27 86. Defendants’ violations of 6 Del. C. § 12B-101, *et seq.* have injured
28 Plaintiffs and August 4 Class members by causing (1) the loss of the unencumbered

1 use of their passwords; (2) the procurement, by hackers, of their Private Information
2 without their consent; and (3) the inability to take steps to protect themselves and their
3 Private Information.

4 87. Defendants' violations of 6 Del. C. § 12B-101, *et seq.* are also violations
5 of the CFA. If Plaintiffs and all other August 4 Class members had been notified,
6 they could have taken precautions to safeguard their Private Information, at least until
7 Defendants froze account holders' ability to amend their Battle.net account details.
8 Since that moment, Defendants have affirmatively, materially impaired Plaintiffs' and
9 all other August 4 Class members' ability to protect their Private Information, and
10 have misrepresented the security of the goods and services they provided and continue
11 to provide to Plaintiffs and all other August 4 Class members.

12 88. Defendants' violations of the CFA have put the Private Information of
13 Plaintiffs and Class members at continual risk. Such behavior, and its attendant
14 consequences, has deprived Plaintiffs and Class members of the full value of all goods
15 and services purchased from Defendants. As the months have unfolded in 2012, and
16 as the instances of reported security lapses mount, it becomes more and more evident
17 that playing games manufactured by Defendants – games that can cost almost \$200 –
18 requires gambling with the sanctity and security of one's Private Information,
19 including, but not limited to, one's name, address, and credit card information. Any
20 game, the playing of which is conditioned upon such a risk, becomes devalued. As
21 the data breaches mount, the value decreases further.

22 89. As a result of Defendants' violations of the CFA, Plaintiffs and all other
23 August 4 Class members are entitled to compensatory damages, including losses
24 sustained in the devaluation of games purchased by Plaintiffs from Defendants, as
25 well as injunctive relief.

COUNT III

Unjust Enrichment

(On Behalf of the Authenticator Class)

90. Plaintiffs repeat all paragraphs above.

91. Plaintiffs and all other Authenticator Class members conferred benefits on Defendants by (1) paying for video games manufactured and developed by Defendants; and (2) signing up for Battle.net accounts.

92. Plaintiffs and all other Authenticator Class members, however, were deprived of the full value of their video games, as well as their Battle.net accounts, due to Defendants' inability to ensure adequate protections for all Private Information entrusted to them by Plaintiffs and all other Authenticator Class members.

93. Where Defendants have suffered data breaches as a result of their own lax security protocols, rather than shouldering the cost of remedying their own error, they required Plaintiffs and Authenticator Class members to purchase a new product – an Authenticator – at additional cost. They did not provide the Authenticator for free or include it with future purchases. Where they should have simply fixed their security protocols without burdening their customers with additional costs, they instead engaged in the extortionate practice of making Plaintiffs and all other Authenticator Class members pay more money for peace of mind.

94. Defendants knowingly and willingly accepted monetary benefits resulting from Plaintiffs' and all other Authenticator Class members' purchases, but failed to honor their obligations to Plaintiffs and all other Authenticator Class members, specifically by failing to abide by the assurances made in their Privacy Policy that all Private Information would be secure, without the acquisition of an Authenticator.

95. Under the circumstances described herein, it is inequitable for Defendants to retain these monetary benefits, derived from Plaintiffs and all other Authenticator Class members.

1 via a Battle.net data breach. Such risk diminishes the value of the game over time,
2 and each successive data breach diminishes a game's value in increasing magnitude.
3 Defendants insist that customers rely on an unsafe website in order to enrich
4 themselves, with the attendant effect of devaluing their customers' purchases.

5 103. Where Defendants have refused to enact sufficient security protocols or
6 to provide notice to customers when data breaches occur, such actions diminish the
7 value of their games over time, and each successive data breach diminishes a game's
8 value in increasing magnitude. Defendants' actions devalue the substantial purchases
9 made by Plaintiffs and members of the August 4 Class, in that they add an increasing
10 and continual level of risk to the act of playing a video game.

11 104. Under the circumstances described herein, it is inequitable for
12 Defendants to retain these monetary benefits, derived from Plaintiffs and all other
13 August 4 Class members.

14 105. By engaging in the conduct described above, Defendants have been
15 unjustly enriched at the expense of Plaintiffs and all other August 4 Class members.
16 Accordingly, it would be contrary to principles of equity and good conscience to
17 permit Defendants to retain any ill-gotten monetary benefits obtained as a result of the
18 actions described herein.

19 106. As a result of Defendants' enrichment, Plaintiffs and all other August 4
20 Class members have suffered injury and are entitled to reimbursement, restitution, and
21 disgorgement by Defendants of the benefit conferred by Plaintiffs and all other August
22 4 Class members.

23 **COUNT V**

24 **Negligence *Per Se***

25 **(On Behalf of the Class)**

26 107. Plaintiffs repeat all paragraphs above.

27 108. Defendants had a duty to timely disclose any incidents of data breaches
28 of Battle.net and Battle.net accounts, where such breaches compromised the Private

1 Information of Plaintiffs and Class members.

2 109. Defendants breached their duty to timely disclose that the Private
3 Information of Plaintiffs and Class members in their possession had been, or was
4 reasonably believed to have been, stolen or compromised.

5 110. Timely disclosure was appropriate so that, among other things, Plaintiffs
6 and Class members could take appropriate measures to avoid unauthorized charges to
7 their credit or debit card accounts; cancel or change usernames or passwords on both
8 compromised accounts and personal accounts utilizing comparable personal or
9 financial information; remove credit or debit card information from their Battle.net
10 accounts; and monitor their account information and credit reports for fraudulent
11 activity.

12 111. But for Defendants' negligent and wrongful breach of their duties of
13 notification owed to Plaintiffs and the Class, Plaintiffs and the Class could have taken
14 remedial measures to protect their Private Information.

15 112. As set forth in paragraphs 82-87, *supra*, Defendants' failure to provide
16 timely notice to Plaintiffs and Class members of Battle.net data breaches are
17 violations of 6 Del. C. § 12B-101, *et seq.*, and are evidence of Defendants' negligence
18 *per se*.

19 113. Where Defendants have negligently failed to provide notice to customers
20 when data breaches occur, such actions diminish the value of their games over time,
21 and each successive data breach diminishes a game's value in increasing magnitude.
22 Defendants' negligence devalues the substantial purchases made by Plaintiffs and
23 members of the Class, in that they add an increasing and continual level of risk to the
24 act of playing a video game.

25 114. Plaintiff and the Class suffered actual damages including, but not limited
26 to: expenses for credit monitoring, anxiety, emotional distress, loss of privacy;
27 diminished value of their video game purchases; and other economic and non-
28 economic harm.

COUNT VI

Negligence

(On Behalf of the Class)

115. Plaintiffs repeat all paragraphs above.

116. Defendants came into possession of Plaintiffs' and Class members' Private Information and had a duty to exercise reasonable care in safeguarding and protecting such information from being compromised and/or stolen.

117. Defendants further had a duty to have procedures in place to detect and prevent the theft or dissemination of the Private Information of Plaintiffs and Class members. This breach of security and unauthorized access was reasonably foreseeable to Defendants, particularly in light of the Battle.net security breaches occurring since at least 2007.

118. Defendants failed to exercise reasonable care in safeguarding and protecting the Private Information of Plaintiffs and Class members by failing to adopt, maintain, and/or implement adequate security measures to prevent data breaches.

119. Defendants had a duty to timely disclose any incidents of data breaches of Battle.net and Battle.net accounts, where such breaches compromised the Private Information of Plaintiffs and Class members.

120. Defendants breached their duty to timely disclose that the Private Information of Plaintiffs and Class members in their possession had been, or was reasonably believed to have been, stolen or compromised.

121. Timely disclosure was appropriate so that, among other things, Plaintiffs and Class members could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts; cancel or change usernames or passwords on both compromised accounts and personal accounts utilizing comparable personal or financial information; remove credit or debit card information from their Battle.net accounts; and monitor their account information and credit reports for fraudulent activity.

122. As set forth in paragraphs 82-87, *supra*, Defendants' failure to provide timely notice to Plaintiffs and Class members of Battle.net data breaches are violations of 6 Del. C. § 12B-101, *et seq.*, and are evidence of Defendants' negligence.

123. But for Defendants' negligent and wrongful breach of their duties owed to Plaintiffs and the Class, their Private Information would not have been compromised.

124. But for Defendants' negligent and wrongful breach of their duties of notification owed to Plaintiffs and the Class, Plaintiffs and the Class could have taken remedial measures to protect their Private Information.

125. Plaintiffs' and the Class's Private Information was compromised, viewed, and/or stolen as the proximate result of Defendants failing to exercise reasonable care in safeguarding such information by adopting, implementing, or maintaining appropriate security measures to protect and safeguard the private, non-public, personal and financial information within their possession.

126. Where Defendants have negligently failed to enact sufficient security protocols or to provide notice to customers when data breaches occur, such actions diminish the value of their games over time, and each successive data breach diminishes a game's value in increasing magnitude. Defendants' negligence devalues the substantial purchases made by Plaintiffs and members of the Class, in that they add an increasing and continual level of risk to the act of playing a video game.

127. Plaintiff and the Class suffered actual damages including, but not limited to: expenses for credit monitoring, anxiety, emotional distress, loss of privacy; diminished value of their video game purchases; and other economic and non-economic harm.

COUNT VII

Breach of Contract

(On Behalf of the Class)

128. Plaintiffs repeat all paragraphs above.

130. Defendants did not safeguard and protect Plaintiffs' and the Class's Private Information from being compromised and/or stolen. Indeed, Defendants allowed this information to be stolen. Defendants subsequently failed to disclose to Plaintiff and the Class that their Private Information had been compromised and/or stolen.

132. Plaintiffs and the Class suffered actual damages including, but not limited to: costs of credit monitoring, diminished value of their video game purchases, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm.

Bailment

133. Plaintiffs repeat all paragraphs above.

135. A bailment arises where possession, but not ownership, of property is

1 transferred from one party (“bailor”) to another (“bailee”). Where a bailee has
 2 received a bailment from a bailor, a duty of care is owed. Typically, a bailee is strictly
 3 liable for the bailment.

4 136. During the period of bailment Defendants, as bailees, owed Plaintiffs and
 5 all other Class members a duty of care to safeguard their Private Information by
 6 maintaining reasonable security procedures and practices to protect such information.
 7 As alleged herein, Defendants breached this duty.

8 137. As a result of Defendants’ breach of this duty, Plaintiffs and all other
 9 Class members have been harmed as alleged herein.

10 **PRAYER FOR RELIEF**

11 WHEREFORE, Plaintiffs seek judgment in favor of themselves and the Class
 12 for the following:

- 13 A. That the Court determine that this action may be maintained as a class
 14 action under Rule 23 of the Federal Rules of Civil Procedure, that
 15 Plaintiffs are proper class representatives; that counsel is adequate Class
 16 Counsel, and that the best practicable notice of this action be given to
 17 members of the Class represented by Plaintiffs;
- 18 B. That judgment be entered against Defendant and in favor of Plaintiffs and
 19 the Class on all of the Causes of Action in this Complaint;
- 20 C. That judgment be entered against Defendants for compensatory damages
 21 in an amount to be determined by a jury at trial, including, but not limited
 22 to, compensatory damages for the cost of an authenticator, the amount in
 23 which the game was devalued, the cost of monitoring Plaintiffs’ and
 24 other Class members’ financial accounts, and making Plaintiffs and the
 25 Class members whole;
- 26 D. That judgment be entered against Defendants for relief in the form of
 27 restitution and disgorgement of Defendants’ unjustly-realized enrichment
 28 in an amount to be determined by a jury at trial;

- 1 E. That judgment be entered against Defendants for injunctive and equitable
2 relief, including, but not limited to: (a) enjoining Defendants from
3 tacking on additional, undisclosed costs to ensure security in the form of
4 a post-point-of-sale Authenticator; (b) enjoining Defendants from
5 requiring customers to acquire a Battle.net account (and thereby risking
6 the security of their Private Information) for game titles that are not
7 MMORPGs, such as the StarCraft or Diablo franchises; and (c) enjoining
8 Defendants from actions which place consumers at a risk of future
9 security breaches;
- 10 F. That judgment be entered against Defendant imposing interest on
11 damages;
- 12 G. That judgment be entered against Defendant imposing litigation costs and
13 attorneys' fees; and
- 14 H. For all other and further relief as this Court may deem necessary and
15 appropriate.

16 Plaintiffs demand a jury trial on all issues so triable.

17
18 DATED: November 5, 2012

Attorneys for Plaintiffs Benjamin Bell,
Christopher Spellman, and the Proposed
Class

19
20
21
22 By: 

23 CARNEY WILLIAMS BATES
24 PULLIAM & BOWMAN, PLLC
Hank Bates

25 MILSTEIN ADELMAN, LLP
26 Gillian L. Wade
27 M. Isaac Miller
28

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge Stephen V. Wilson and the assigned discovery Magistrate Judge is Patrick J. Walsh.

The case number on all documents filed with the Court should read as follows:

CV12- 9475 SVW (PJWx)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

=====

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

☒ **Western Division**
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

☐ **Southern Division**
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

☐ **Eastern Division**
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.

MILSTEIN ADELMAN, LLP
 Gillian L. Wade, State Bar No. 229124
 M. Isaac Miller, State Bar No. 266459
 2800 Donald Douglas Loop North
 Santa Monica, CA 90405
 Tel: 310-396-9600

COPY

UNITED STATES DISTRICT COURT
 CENTRAL DISTRICT OF CALIFORNIA

BENJAMIN BELL and CHRISTOPHER
 SPELLMAN,

PLAINTIFF(S)

v.

BLIZZARD ENTERTAINMENT,
 INC., a Delaware corp., and ACTIVISION
 BLIZZARD, INC., a Delaware corp.

DEFENDANT(S).

CASE NUMBER

CV12-09475 SVW (PJW x)

SUMMONS

TO: DEFENDANT(S):

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it), you must serve on the plaintiff an answer to the attached ☒ complaint ☐ amended complaint ☐ counterclaim ☐ cross-claim or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff's attorney, Gillian L. Wade, whose address is 2800 Donald Douglas Loop North, Santa Monica, CA 90405. If you fail to do so, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

NOV - 5 2012

Dated: _____

Clerk, U.S. District Court

JULIE PRADO

By: _____

Deputy Clerk

(Seal of the Court)

[Use 60 days if the defendant is the United States or a United States agency, or is an officer or employee of the United States. Allowed 60 days by Rule 12(a)(3)].

COPYUNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

I (a) PLAINTIFFS (Check box if you are representing yourself <input type="checkbox"/>) BENJAMIN BELL and CHRISTOPHER SPELLMAN,	DEFENDANTS BLIZZARD ENTERTAINMENT, INC., a Delaware corp., and ACTIVISION BLIZZARD, INC., a
(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.) MILSTEIN ADELMAN, LLP, Gillian L. Wade/ M. Isaac Miller 2800 Donald Douglas Loop North, Santa Monica, CA 90405 Telephone: 310-396-9600	Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an X in one box only.) <input type="checkbox"/> 1 U.S. Government Plaintiff <input type="checkbox"/> 3 Federal Question (U.S. Government Not a Party) <input type="checkbox"/> 2 U.S. Government Defendant <input checked="" type="checkbox"/> 4 Diversity (Indicate Citizenship of Parties in Item III)	III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only (Place an X in one box for plaintiff and one for defendant.) <table style="width:100%;"> <tr> <th></th> <th>PTF</th> <th>DEF</th> <th></th> <th>PTF</th> <th>DEF</th> </tr> <tr> <td>Citizen of This State</td> <td><input type="checkbox"/> 1</td> <td><input type="checkbox"/> 1</td> <td>Incorporated or Principal Place of Business in this State</td> <td><input type="checkbox"/> 4</td> <td><input type="checkbox"/> 4</td> </tr> <tr> <td>Citizen of Another State</td> <td><input checked="" type="checkbox"/> 2</td> <td><input type="checkbox"/> 2</td> <td>Incorporated and Principal Place of Business in Another State</td> <td><input type="checkbox"/> 5</td> <td><input checked="" type="checkbox"/> 5</td> </tr> <tr> <td>Citizen or Subject of a Foreign Country</td> <td><input type="checkbox"/> 3</td> <td><input type="checkbox"/> 3</td> <td>Foreign Nation</td> <td><input type="checkbox"/> 6</td> <td><input type="checkbox"/> 6</td> </tr> </table>		PTF	DEF		PTF	DEF	Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	<input type="checkbox"/> 4	<input type="checkbox"/> 4	Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 5	Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6
	PTF	DEF		PTF	DEF																				
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business in this State	<input type="checkbox"/> 4	<input type="checkbox"/> 4																				
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business in Another State	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 5																				
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6																				

IV. ORIGIN (Place an X in one box only.)
☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify): ☐ 6 Multi-District Litigation ☐ 7 Appeal to District Judge from Magistrate Judge

V. REQUESTED IN COMPLAINT: JURY DEMAND: ☒ Yes ☐ No (Check 'Yes' only if demanded in complaint.)
CLASS ACTION under F.R.C.P. 23: ☒ Yes ☐ No **MONEY DEMANDED IN COMPLAINT:** \$ TBD at Trial

VI. CAUSE OF ACTION (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)
 Delaware's Consumer Fraud Act ("CFA") 6 Del. C. § 2511 et seq.

VII. NATURE OF SUIT (Place an X in one box only.)

OTHER STATUTES <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce/ICC Rates/etc. <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 810 Selective Service <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 875 Customer Challenge 12 USC 3410 <input checked="" type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Act <input type="checkbox"/> 892 Economic Stabilization Act <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 894 Energy Allocation Act <input type="checkbox"/> 895 Freedom of Info. Act <input type="checkbox"/> 900 Appeal of Fee Determination Under Equal Access to Justice <input type="checkbox"/> 950 Constitutionality of State Statutes	CONTRACT <input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loan (Excl. Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise REAL PROPERTY <input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	TORTS PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Fed. Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury-Med Malpractice <input type="checkbox"/> 365 Personal Injury-Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability IMMIGRATION <input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 463 Habeas Corpus-Alien Detainee <input type="checkbox"/> 465 Other Immigration Actions	TORTS PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability BANKRUPTCY <input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 CIVIL RIGHTS <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 444 Welfare <input type="checkbox"/> 445 American with Disabilities - Employment <input type="checkbox"/> 446 American with Disabilities - Other <input type="checkbox"/> 440 Other Civil Rights	PRISONER PETITIONS <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 Habeas Corpus General <input type="checkbox"/> 535 Death Penalty <input type="checkbox"/> 540 Mandamus/Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition FORFEITURE/PENALTY <input type="checkbox"/> 610 Agriculture <input type="checkbox"/> 620 Other Food & Drug <input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 630 Liquor Laws <input type="checkbox"/> 640 R.R. & Truck <input type="checkbox"/> 650 Airline Regs <input type="checkbox"/> 660 Occupational Safety/Health <input type="checkbox"/> 690 Other	LABOR <input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Mgmt. Relations <input type="checkbox"/> 730 Labor/Mgmt. Reporting & Disclosure Act <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Empl. Ret. Inc. Security Act PROPERTY RIGHTS <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 840 Trademark SOCIAL SECURITY <input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g)) FEDERAL TAX SUITS <input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS-Third Party 26 USC 7609
--	--	--	---	---	---

CV12-09475

FOR OFFICE USE ONLY: Case Number: _____

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

**UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET**

VIII(a). IDENTICAL CASES: Has this action been previously filed in this court and dismissed, remanded or closed? ☒ No ☐ Yes
If yes, list case number(s): _____

VIII(b). RELATED CASES: Have any cases been previously filed in this court that are related to the present case? ☒ No ☐ Yes
If yes, list case number(s): _____

Civil cases are deemed related if a previously filed case and the present case:

- (Check all boxes that apply) ☐ A. Arise from the same or closely related transactions, happenings, or events; or
☐ B. Call for determination of the same or substantially related or similar questions of law and fact; or
☐ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
☐ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

IX. VENUE: (When completing the following information, use an additional sheet if necessary.)

- (a) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named plaintiff resides.
☐ Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles, California	Little Rock, Arkansas

- (b) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named defendant resides.
☐ Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
	Delaware

- (c) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** claim arose.
Note: In land condemnation cases, use the location of the tract of land involved.

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles, California	

* Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties

Note: In land condemnation cases, use the location of the tract of land involved

X. SIGNATURE OF ATTORNEY (OR PRO PER):  Date November 5, 2012

Notice to Counsel/Parties: The CV-71 (JS-44) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))